UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Richmond Division

MARSHA HEATH, SHERRY BLACKBURN, ISABEL DELEON, ASHLEY GRANT, and LEANA YANCEY, *individually and on behalf of all others similarly situated,*

Plaintiffs,

v.

Case No. 3:19cv555

Capital One Financial Corporation, Capital One, N.A. and Capital One Bank (USA),

Defendants.

CLASS ACTION COMPLAINT

COME NOW Plaintiffs, Marsha Heath, Sherry Blackburn, Isabel DeLeon, Ashely Grant, and Leana Yancey, *on behalf of themselves and all individuals similarly situated* ("Plaintiffs"), by counsel, and for their Class Action Complaint against Defendants Capital One Corporation, Capital One, N.A., and Capital One Bank (USA) (collectively "Capital One"), allege as follows:

NATURE OF THE ACTION

1. This case arises from Capital One's failure to exercise basic, reasonable care in securing and safeguarding what is among the most-valuable things consumers possess—their sensitive personal information. Through its failure to secure, monitor, and protect information that consumers provided to Capital One at its insistence when they applied for credit, Capital One permitted an individual to commit one of the largest data breaches on record.

2. Capital One's lackadaisical approach to data security permitted an individual to obtain and post on the Internet reams of data with which consumers like Plaintiffs entrusted

Capital One, including their full names, addresses, phone numbers, dates of birth, credit scores, credit limits, account information, account balances, payment histories, Social Security Numbers ("SSNs"), and bank account numbers (together known as "personal identifying information" or "PII").

3. Plaintiffs, individually and on behalf of similarly situated consumers, seek to recover damages; equitable relief, including injunctive relief designed to prevent a reoccurrence of the Data Breach and resulting injuries; restitution; disgorgement; reasonable costs and attorneys' fees; and all other remedies this Court deems proper.

PARTIES

4. Marsha Heath is a Virginia resident who resides in this District and Division.

5. Plaintiff Sherry Blackburn is a Virginia resident who resides in this District and Division.

6. Plaintiff Isabel DeLeon is a Virginia resident who resides in this District and Division.

7. Plaintiff Ashley Grant is a Virginia resident who resides in this District and Division.

8. Plaintiff Leana Yancey is a Virginia resident who resides in this District and Division.

9. Defendant Capital One Financial Corporation is a Delaware corporation with its principal place of business located in the Richmond, Virginia region. Capital One Financial Corp. operates through its two primary subsidiaries, also Defendants here, Capital One Bank (USA) and Capital One, N.A.

10. Capital One Bank (USA), National Association is a subsidiary of Capital One Financial Corporation.

11. Capital One, National Association is a subsidiary of Capital One Financial Corporation.

JURISDICTION AND VENUE

12. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) because sufficient diversity of citizenship exists between parties in this action, the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, and there are 100 or more members of the Class because Capital One has estimated that 100,000,000 consumers were affected by the Data Breach.

13. At least one member of the proposed Class is diverse in citizenship from Capital One. 28 U.S.C. § 1332(d)(2)(A).

14. The Court has personal jurisdiction over Capital One because its principal place of business is in the Eastern District of Virginia and in the Richmond Division, and Capital One is authorized to and regularly conducts business in this District and Division.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Capital One is a corporation, has its principal place of business in this District, and a substantial part of the events and omissions giving rise to this action occurred in this District and Division.

FACTUAL ALLEGATIONS

A. The Banking System Is A Known, Constant Target For Criminals.

16. Data breaches have become widespread, with almost-daily notices of their occurrence. The Identity Theft Resource Center publishes reports showing thousands of such breaches over the past three years.

17. News sources confirm that "[t]he risk of cyberattack on financial services firms cannot be overstated" as financial services companies like Defendants "fall victim to cybersecurity attacks 300 times more frequently than businesses in other industries."[1] Not surprisingly, then, "financial institutions have long been a lucrative target for cybercriminals because of the massive volumes of data and money that can be stolen."[2]

18. The consequences to consumers from companies' lax data supervision and safety are significant, as sensitive personal and financial information is exposed often without anyone's knowledge, most-importantly the entities that should be safeguarding that information. It is further exacerbated where, like here, compromised information includes PII and SSNs, which then makes it possible for thieves to open new credit accounts, obtain licenses and other certifications, apply for mortgages and housing, file for unemployment benefits, access retirement or savings accounts, or apply for a job using a false identity.

19. Each of these acts or fraud is difficult to detect and may not be uncovered until the SSN has been used in a fraudulent transaction of which the owner of the PII somehow becomes aware.

20. Significantly, it is no easy feat to change or cancel a compromised SSN, if it can be done at all. Even then, a new SSNs may not be any solution, as consumer reporting agencies get confused by conflicting SSNs such that they often link new SSNs to the original consumer, so the data tied to the old number is again connected to the original consumer after fraud has occurred.

---

[1] Forbes, *Laughing All The Way To The Bank: Cybercriminals Targeting U.S. Financial Institutions*, Aug. 28, 2018, available at https://www.forbes.com/sites/bhaktimirchandani/2018/08/28/laughing-all-the-way-to-the-bank-cybercriminals-targeting-us-financial-institutions/#68b8a01f6e90.

[2] Help Net Security, Increasing number of financial institutions falling prey to cyber attacks, Nov. 9, 2016, *available at* hnps://www.helpnetsecurity.co m/2016/11/09/financial-institutions-cyber-attacks/, last visited July 31, 2019.

21. Capital One knew the importance of safeguarding PII entrusted to it and of the foreseeable consequences if its data security systems were to be breached, including the significant costs that would be imposed on consumers as a result of a breach.

22. Yet, Capital One put its own profits ahead of its responsibilities to consumers, cutting security corners and failing to place enough emphasis on the safeguarding and monitoring of PII with which consumers like Plaintiffs entrusted it.

B. Capital One's Consumer Data Collection Practices And Its Knowledge Of The Value Of Such Data In The Wrong Hands.

23. As part of applying for a credit card and other financial products and services, consumers provide banks like Capital One their names, addresses, SSNs, and other valuable, sensitive, and private PII.

24. At all times relevant to the Data Breach, Capital One was well-aware, or reasonably should have been aware, that the PII collected, maintained, and stored from credit applications is highly sensitive, sought after by criminals, susceptible to attack, and could be used for wrongful purposes—like identity theft and fraud—by third parties.

25. Banking repositories and databases are popular targets for cyberattacks, especially given the extremely sensitive nature of the PII stored on those repositories and databases. The frequency and prevalence of attacks make it imperative that banks such as Capital One routinely monitor for exploits and intrusions, security lapses, software changes, and cyberattacks, and regularly update their software and security procedures.

26. Security lapses, intrusions, and software exploits can go undetected for long periods of time, especially if industry best practices are not routinely instituted and followed to maintain data security.

27. PII is a valuable commodity and can be readily traded. An Internet black market exists in which criminals openly post stolen payment card numbers, SSNs, and other PII on underground Internet websites. PII is valuable to identity thieves because they can use victims' personal data to open new financial accounts, take out loans or otherwise obtain credit or goods in another person's name, incur charges on existing accounts, invade and pilfer bank accounts, or clone ATM, debit, and credit cards.

28. Such is especially true for banks like Capital One, given that the PII disclosed in this Data Breach was precisely the PII Capital One requested to consider and, in many cases, approve consumers for credit cards and other banking products. Put differently, the PII that Capital One used to permit Plaintiffs to open accounts could be put to equal use by fraudsters for the same purpose.

29. Given that Capital One demanded the PII, it should have had a heightened awareness of its need to protect the PII with which consumers entrusted it.

30. Professionals charged with trying to stop fraud and other misuse know that PII has genuine monetary value in part because criminals make great efforts to obtain it.[3] In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminals' efforts to obtain such data. On the contrary, just the opposite has occurred. For example, the Identity Theft Resource Center reported 1,579 data breaches in 2017, which represents a 44.7 percent increase over the record high figures reported for 2016.[4]

---

[3] CIO Magazine, *Data Breaches Rise as Cybercriminals Continue to Outwit IT* (Oct. 2016), *available at* https://www.cio.com/article/2686167/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html (last visited July 31, 2019).

[4] *2017 Annual Data Breach Year-End Review*, ID Theft Center (2017), *available at* https://www.idtheftcenter.org/data-breaches/ (last visited July 31, 2019).

31. The PII of consumers remains of high value to identity thieves, as evidenced by the prices criminals will pay through black-market sources, otherwise known as the "dark web." For example, a complete set of bank account credentials can fetch a thousand dollars or more, depending on the associated credit score or balance available.[5] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[6]

32. At all relevant times, Capital One knew, or reasonably should have known, of the importance of safeguarding PII, and should have foreseen the consequences if its data security was breached, including, specifically, the significant costs that would be imposed on consumers.

33. Capital One was, or should have been, fully aware of the significant volume of daily online credit applications, amounting to tens of thousands of daily interactions with consumers' PII, and thus, the significant number of individuals who would be harmed by a breach of Capital One's systems.

34. Sadly, and as alleged herein, despite all of this publicly available knowledge of the need to keep PII secure because of the constant threat of breaches, and the supposed expertise it had or could have devoted to ensure data security, Capital One's approach to maintaining the privacy and security of Plaintiffs and Class Members' PII was lackadaisical, cavalier, reckless, or at the very least, negligent.

C. Plaintiffs' Entrustment Of Their PII To Capital One.

35. Plaintiff Sherry Blackburn opened a Capital One credit card account in May 2015. She also opened a credit card with retailer Kohl's in August 2012. Capital One services credit card

---

[5] *Here's How Much Thieves Make By Selling Your Personal Data Online*, Business Insider, *available at* https://www.businessinsider.com/heres-how-much-your-personal-data-costs-on-the-dark-web-2015-5, May 27, 2015 (last visited July 31, 2019).

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web, available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited July 31, 2019).

accounts for Kohl's.

36. Plaintiff Isabel DeLeon applied for a Capital One credit card in May 2015, which Capital One denied.

37. Plaintiff Ashley Grant opened two Capital One credit card accounts, one in November 2002 that she closed in November 2007, and one in October 2015 that remains open.

38. Plaintiff Leana Yancey was the victim of Identity Theft and as a result, two false applications were submitted to Capital One in April 2015 containing her PII, and both remain open.

39. Plaintiff Marsha Heath opened a Capital One credit card account in April 2013.

40. In each instance as above, the PII of Plaintiffs was provided to Capital One.

41. Since the announcement of the Data Breach, Plaintiffs must now monitor their accounts in an effort to detected and prevent any misuse of their PII or improper activity. Each has had to personal and work time attempting to determine the impact of this breach on their financial privacy and safety.

42. Plaintiffs must spend time to protect the integrity of their information, finances, and credit—time which she would not have had to expend but for the Data Breach.

43. Plaintiffs would not have applied for credit with and provided PII to Capital One had Capital One disclosed that it lacked adequate computer systems, monitoring programs, and data security practices to safeguard consumers' PII from improper access.

44. Plaintiffs suffered actual injury from having their PII stolen and published as a result of the Data Breach.

45. Plaintiffs suffered concrete injury and actual damages in paying money to, and purchasing products through, Capital One's business preceding, during, and after the Data Breach by paying interest on credit cards, paying minimum balance fees, and other banking fees.

46. Plaintiffs would not have incurred these expenditures with Capital One had Capital One disclosed that it lacked computer systems, monitoring programs, and data security practices adequate to safeguard consumers' PII.

47. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII—a form of intangible property that the Plaintiff entrusted to Capital One for the purpose of applying for and using Capital One's products, which was compromised in and as a result of the Data Breach.

48. Plaintiffs have suffered additional injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

49. Plaintiffs have a continuing interest in ensuring their PII, which remains in the possession of Capital One, is protected and safeguarded from future breaches.

D. The Data Breach.

50. On July 29, 2019, Capital One admitted to one of the largest data breaches in history, in which more than 100 million US consumers were affected. [7] The Data Breach notice stated in relevant part:

> Capital One Announces Data Security Incident
>
> * * *
>
> MCLEAN, Va., July 29, 2019 /PRNewswire/ -- Capital One Financial Corporation (NYSE: COP) announced today that on July 19, 2019, it determined there was unauthorized access by an outside individual who obtained certain types of personal information relating to people who had applied for its credit card products and to Capital One credit card customers.

---

[7] Date Breach Notice, FAQ (July 29, 2019), *available at* https://www.capitalone.com/facts2019/(hereinafter the "Breach Notification") (last visited July 31, 2019).

* * *

Based on our analysis to date, this event affected approximately 100 million individuals in the United States and approximately 6 million in Canada.

* * *

The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019. This information included personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income. Beyond the credit card application data, the individual also obtained portions of credit card customer data, including:

- Customer status data, e.g., credit scores, credit limits, balances, payment history, contact information
- Fragments of transaction data from a total of 23 days during 2016, 2017 and 2018.

* * *

- About 140,000 Social Security numbers of our credit card customers
- About 80,000 linked bank account numbers of our secured credit card customers

* * *

We will notify affected individuals through a variety of channels. We will make free credit monitoring and identity protection available to everyone affected.

Safeguarding our customers' information is essential to our mission and our role as a financial institution. We have invested heavily in cybersecurity and will continue to do so. We will incorporate the learnings from this incident to further strengthen our cyber defenses.

For more information about this incident and what Capital One is doing to respond, visit www.capitalone.com/facts2019. In Canada, information can be found at www.capitalone.ca/facts2019 and www.capitalone.ca/facts2019/fr. The investigation is ongoing and analysis is subject to change. As we learn more, we will update these websites to provide additional information.[8]

[8] *Capital One Announces Data Security Incident*, Cision PR Newswire ("Data Security Article"), *available at* https://www.prnewswire.com/news-releases/capital-one-announces-data-security-

51. Confirming its failure to monitor its data security, the massive breach went undiscovered by Capital One despite the fact that the alleged data thief - Thompson - had posted publicly about the breach on social media accounts over the course of several months and Capital One had records showing the unauthorized intrusion.[9] Moreover, Capital One—which has virtually unlimited resources to protect the vulnerable data with which it is entrusted—was fully aware of the perils of a data breach and its legal responsibility to protect against a data breach, acknowledging in a recent public filing that "[s]afeguarding our customers' information is essential to our mission as a financial institution."[10]

52. The exposed information includes names, addresses, zip codes, phone numbers, email addresses, dates of birth, self-reported income, approximately 140,000 Social Security Numbers, 80,000 bank account numbers, credit scores, credit limits, credit card balances, credit card payment history, and fragments of transaction data from 23 days during 2016, 2017, and 2018. Capital One represented that the data was encrypted but that the unauthorized access "also enabled the decrypting of [the] data."[11]

53. The Capital One Data Breach occurred because Capital One failed to secure the PII of approximately 100 million consumers in Capital One's cloud-based repository and database.[12]

54. Separately from Capital One's initial inability or failure to prevent the Data Breach, Capital One also failed to detect the breach for approximately three months. Discovery will show

---

incident-300892738.html (last visited July 31, 2019).

[9] Krebs on Security, *Capital One Data Theft Impacts 106M People* (July 30, 2019), *available at* https://krebsonsecurity.com/2019/07/capital-one-data-theft-impacts-106m-people/.

[10] Capital One's July 29, 2019 Form 8-K, *available at* http://phx.corporate-ir.net/phoenix.zhtml?c=70667&p=irolSECText&TEXT=aHR0cDovL2FwaS50ZW5rd2l6YXJkLmNvbS9maWxpbmcueG1sP2lwYWdlPTEzMDI4NzA4JkRTRVE9MCZTRVE9MCZTUURFU0M9U0VDVElPTl9FTlRJUkUmc3Vic2lkPTU3 (last visited August 1, 2019).

[11] July 30 Form 8-K.

[12] Breach Notification.

the posted PII of approximately 100 million consumers on Thompson's GitHub account remained exposed until at least July 17, 2019, when an unidentified tipster informed Capital One of the posting by emailing the bank a warning and a link to the GitHub address.

55. The Data Breach was the result of Capital One's inadequate and lackadaisical approach to data security and protection of PII with which consumers entrusted it during the course of its business. The deficiencies in Capital One's data security were so significant that the misconfigured firewall permitted access to any consumer or small business that applied for one of Capital One's credit card products from 2005 through early 2019—fourteen years of data left unprotected and exposed for any malicious actor to access, view, download, and exploit.[13]

56. Capital One reported that the Data Breach impacted consumers who applied for Capital One credit card products from 2005 through "early 2019," with information that included "personal information Capital One routinely collects at the time it receives credit card applications, including names, addresses, zip codes/postal codes, phone numbers, email addresses, dates of birth, and self-reported income."[14]

57. In addition to its "routine" collections, Capital One also admitted consumers' credit scores, credit limits, balances, payment histories, contact information, and "fragments of transaction data from a total of 23 days during 2016, 2017 and 2018" were accessed.[15]

58. Capital One further admitted that "about 140,000 Social Security numbers of [its] credit card customers" and "about 80,000 linked bank account numbers of our secured credit card customers" were also disclosed.[16]

---

[13] Breach Notification.
[14] *Id.*
[15] *Id.*
[16] *Id.*

59. At no point did Capital One offer any concrete assistance or offer to remunerate Plaintiffs or the Class for its failures. Despite acknowledging that the PII was stolen by a malicious actor and placed on the Internet for anyone to access, view, download, and use, Capital One attempted to downplay the gravity of the breach, claiming "it is unlikely that the information was used for fraud or disseminated by this individual."[17]

60. And so the misrepresentations have begun. Capital One knows the last portion of this statement is demonstrably false, as Ms. Thompson disseminated the PII she obtained throughout the Internet, posting it on a public site for all to see.[18]

61. As alleged in the federal criminal complaint against her, the file posted by Thompson contained the IP address for a server at Amazon Web Services, which provides computing services to Capital One. The file also contained command information permitting access to data in Capital One's storage space at the cloud computing company. A firewall misconfiguration permitted the commands to reach and be executed by Amazon's server, thereby enabling unauthorized access to the Capital One data.[19]

62. The file Thompson posted contained "700 folders or buckets of data," as well as code for three commands that could be used to obtain the data. The three commands, when executed, performed as follows:

---

[17] Data Security Article.

[18] Merriam-Webster defines disseminate as "to spread abroad as though sowing seed," and "to disperse throughout." https://www.merriam-webster.com/dictionary/disseminate.

[19] *United States v. Paige A. Thompson, a/k/a "erratic"*, No. 2:19-mj-00344-MAT (W.D. Wash.), ECF 1 ¶¶ 7–10 (filed July 29, 2019) (the "Thompson Complaint"), *available at* https://www.justice.gov/usao-wdwa/press-release/file/1188626/download (last visited Aug. 1, 2019).

a. The first command obtained security credentials for an account known as WAF-Role that enabled access to certain of Capital One's folders at the cloud computing company;

b. The second command used the WAF-Role account to list the names of folders or buckets of data in Capital One's storage space at the cloud computing company; and,

c. The third command then used the same account the extract or copy data from the folders or buckets in Capital One's storage space for which the account had permissions.[20]

63. Capital One tested the three commands and confirmed that the commands functioned to obtain Capital's One credentials and could be used to extract data.[21]

64. Further, as alleged in the Thompson criminal complaint, Capital One's logs show a number of connections or attempted connections to Capital One's server from an Onion Router (or "TOR"), a tool used by individuals to conceal their identities and the origin of their internet connection (or IP address), and a number of connections from a specific IP address beginning with 46.246, all of which Capital One believes relate to activity conducted by the same person involved in the April 21, 2019 intrusion.

65. In Capital One's Form 8-K disclosing the Data Breach, Capital One confirmed that unauthorized activity occurred on March 22 and 23, 2019.

66. The FBI's investigation revealed that after completing the hack, Thompson created a Meetup group with a Slack invitation for a public Slack channel. Meetup is an internet-based platform designed to let people find and build local communities, and Slack is a cloud-based team-

[20] *Id.* ¶ 11.
[21] *Id.* ¶ 12.

collaboration software tool where users can establish "channels" in which they can then share messages, tools, and files.[22]

67. On the publicly-accessible Slack channel created by Thompson, a user named "erratic"—which the FBI alleges is Thompson—posted a list of files the user claimed to possess, which included files that were extracted using the commands set forth in the April 21st Github file posted by Thompson.[23]

68. Around June 27, 2019, according to the FBI, "erratic posted [on the Slack channel] about several companies, government entities, and educational institutions, and included in the post references to the April 21st Github files associated with Capital One. After this posting, another user posted "don't go to jail plz" to which "erratic" responded "Im like > ipredator > tor > s3 on all this [expletive]." The FBI interpreted this response to be detailing the method "erratic" used to commit the intrusion, that Ms. Thompson used IPredator and TOR to conceal her IP address.[24]

69. Investigative Reporter Brian Krebs, who operates the website Krebs on Security, reported that Thompson spoke openly on her Twitter account over the course of several months about finding huge stores of data intended to be secured on various Amazon cloud servers—the servers from which (he suggested) Thompson likely stole the Capital One data.[25]

70. Capital One's failure to detect the breach sooner is even more shocking given the public nature of Thompson's disclosures. As Krebs explains, "[i]ncredibly, much of this breach played out publicly over several months on social media and other open online platforms" such as

---

[22] *Thompson* Complaint ¶ 17.
[23] *Id.* ¶ 18.
[24] *Id.* ¶¶ 19–20.
[25] Krebs on Security, Capital One Data Theft Impacts 106M People (July 30, 2019).

Twitter, Meetup, and Slack. And, for months beginning in April 2019, Capital One's stolen data and the means to access, view, and obtain were available, in the open, on Github.

71. This PII was compromised due to Capital One's acts and omissions and its failure to properly protect the PII, despite being aware of cybersecurity dangers, the necessary standards, industry best practices, and the vulnerability of financial service institutions to attack.

72. Apart from its failure to prevent the Data Breach, Capital One also failed to detect the breach for at least three months—despite it being publicly represented on the popular and oft-trafficked GitHub website. Anyone with Internet access therefore had at least three months to access, view, collect, download, and make use of this information for fraudulent and other malicious purposes.

73. During this period, Capital One failed to recognize its systems had been breached and that individuals were stealing the PII of 100 million credit card applicants. Indeed, the Breach was not even discovered as a result of Capital One's diligence or cyber security measures but, rather, by a third party who sent a message to a company email address with a link to the GitHub page. Without that tip, Capital One would likely never have learned of the Breach on its own.

74. While timely action by Capital One in identifying the Breach would likely have significantly reduced the harmful consequences, Capital One's inaction and negligence contributed to and only increased the scale of the Data Breach and the resulting damages to Plaintiff and Class Members.

E. Capital One's Inadequate Privacy Policies And Agreements To Keep PII Confidential.

75. As a condition of credit, Capital One required applicants to provide it with PII. In its ordinary business, Capital One maintained and used this PII as a means of deciding whether to extend credit to applicants like Plaintiffs.

76. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and the Class Members' PII, Capital One assumed legal and equitable duties to those individuals. Having been provided Plaintiffs' and Class Members' PII as a result of its demands, Capital One knew or should have known it was responsible for protecting that PII. At all relevant times, Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have disclosed it to Capital One had they known Capital One would fail to protect it.

77. As credit applicants to Capital One, Plaintiffs and the Class Members relied on and reasonably expected Capital One to keep their PII confidential and securely maintained, to use this information only for purposes they authorized, and to make only authorized disclosures of this information.

78. In addition to its obligations under the law when it obtained the PII it demanded, Capital One independently and routinely promised to safeguard PII:

> To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.[26]

> Capital One understands how important security and confidentiality are to our customers, so we use the following security techniques, which comply with or even exceed federal regulatory requirements to protect information about you.[27]

> **Information Security**
> At Capital One, we make your safety and security a top priority and are committed to protecting your personal and financial information. If we collect identifying information from you, we will protect that information with controls based upon internationally recognized security standards, regulations, and industry-based best practices.[28]

F. Capital One Failed to Comply with Federal Requirements.

[26] https://www.capitalone.com/bank/privacy/
[27] https://www.capitalone.com/identity-protection/privacy/faq.
[28] https://www.capitalone.com/identity-protection/privacy/statement.

79. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decisions.[29]

80. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established fundamental data security principles and practices for business.[30] These guidelines note, among other things, businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

81. The FTC guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

82. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on networks; and verify that third-party service providers have implemented reasonable security measures.[31]

83. Also, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an

---

[29] Fed. Tr. Comm'n, *Start With Security*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[30] Fed. Tr. Comm'n, *Protecting Personal Information: A Guide for Business*, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf. [sic].
[31] FTC, Start With Security, *supra* note 32.

unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

84. Capital One's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data like PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

85. Here and as it relates to the Data Breach, Capital One was at all times fully aware of its obligation to protect the PII of its applicants because of its existence a one of the United States' largest financial institutions, the resources it possesses, and the access to information it has. Its own public filings, noted herein, confirm that Capital One knew of the risks of the failure to adequately protect PII in its trust, yet it soldiered on.

86. Capital One was also aware of the significant impact if it failed to protect PII because it demanded such data from millions of consumers daily and knew that this data, if accessed improperly, would result in injury to consumers like Plaintiffs and Class Members.

G. The Data Breach Caused Harm And Will Result In Additional Fraud.

87. The implications of Capital One's failure to keep consumers' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

88. It is no surprise that consumer victims of data breaches are more likely to become victims of identity fraud. This conclusion is bolstered by research like a published analysis of four years of data comparing the numbers of breach victims with those who also reported being victims of identity fraud.[32]

---

[32] 2014 LexisNexis True Cost of Fraud Study, https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

89. In its published materials, the FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[33] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[34]

90. PII is a known valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have PII, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[35]

91. Identity thieves can use PII like that which Capital One failed to keep secure to engage in all matters of nefarious activity. Identity thieves are known to commit various types of government fraud such as: immigration fraud, tax-refund fraud, licensing fraud, benefits fraud.

92. Capital One's delay in detecting and notifying consumers of the Data Breach increases the risk of fraud for Plaintiff and Class Members.

93. A 2016 survey of 5,028 consumers confirms this, as it found "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[36]

---

[33] 17 C.F.R § 248.201(b)(9) (2013).
[34] *Id.* § 248.201(b)(8).
[35] Fed. Tr. Comm'n, *Warning Signs of Identity Theft*, *available at* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited July 31, 2019).
[36] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new.

94. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the six years preceding 2016.

95. Further, simply reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. Rather, identity theft victims must spend numerous hours, if not days, and their own money searching for, finding, and repairing the negative impact to their lives. The Department of Justice's Bureau of Justice Statistics found that in 2014 identity theft victims expended seven hours discovering and resolving the consequences of fraud.

96. A study conducted for BillGuard, a private enterprise that markets its ability to automate the task of finding unauthorized consumer transactions that might otherwise go undetected, calculated the average per-consumer cost of all unauthorized transactions at roughly $215 per cardholder, some portion of which likely goes unnoticed and thus must be paid entirely by consumer victims of account or identity misuse.

97. As a direct and proximate result of Credit One's wrongful conduct and omissions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing harm as well as increased risk of harm from identity theft and fraud.

98. Plaintiffs and the Class are therefor are faced with an arduous path to secure their PII and regain their privacy because of Capital One's negligence. Plaintiffs and the Class must take at least the following steps to attempt to prevent further misuse of their PII:

a. Continually review and monitor credit card statements for any unusual or unknown charges;

b. Review other accounts including savings and retirement accounts, government benefits accounts, mortgage accounts, to name a few, for unauthorized activity;

c. Contact their financial institution (which may not be Capital One) to determine if there is any suspicious activity on their accounts;

d. Review and monitor their credit reports for suspicious activity and accuracy;

e. Change their account information, if not their banks;

f. Place a fraud alert on their credit reports; and

g. Place a security freeze on their credit reports.

99. Additionally, there is usually a period of time between when harm occurs and when it is discovered, as well as between when PII is stolen and when it is used. The Government Accountability Office notes that in some instances, up to a year can pass before stolen data is used to commit identity theft. And once compromised data is posted on the Internet, unauthorized use may continue for years. It is therefore difficult, if not impossible, to rule out all likelihood of future harm from data breaches.

100. There remains a very strong probability that those impacted by Capital One's failure to secure their PII could be at risk of fraud and identity theft for extended periods of time.

101. Thus, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, bank accounts, financial records, and the like. Plaintiffs and the Class are incurring and will continue to incur such damages in addition to any fraudulent credit and debit card charges incurred using their PII and the resulting loss of use of their credit and access to funds, regardless of whether such charges are ultimately reimbursed by banks and credit card companies.

H. Plaintiffs' And Class Members' Damages.

102. The PII is private, personal, and sensitive in nature and was left inadequately protected by Capital One. Capital One did not obtain Plaintiffs' and Class Members' consent to disclose their PII to any other person as required by applicable law and industry standards.

103. The Data Breach was a direct and proximate result of Capital One's failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use,

and disclosure, as required by various state and federal regulations, industry practices, and the common law.

104. This unauthorized access resulted from Capital One's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII to protect against reasonably foreseeable, known threats to the security of such information.

105. Capital One had the resources to prevent the Breach, but instead chose to put profit ahead of consumers' privacy and protection of consumers' PII.

106. Had Capital One monitored, discovered, and remedied the deficiencies in its computer systems, followed federal and state guidelines, and adopted security measures recommended by experts in the field, Capital One would have prevented intrusion into its computer systems and, ultimately, the theft of consumers' confidential PII with which it was entrusted.

107. As a result of Capital One's wrongful actions, inaction, negligent security practices, and the resulting Data Breach, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other pursuits such as work and family.

108. Instead, they must make constant and vigilant efforts to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, changing banks, carefully reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time, and time they will expend, has been lost forever and cannot be recaptured.

109. Capital One's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including for example:

a. outright theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the impending injury from potential fraud and identity theft posed by their PII being placed in the hands of criminals and misused via the sale of PII on the Internet's black market;

d. the untimely and inadequate notification of the Data Breach, which exacerbated all measures of damages;

e. the improper, public disclosure of their PII;

f. invasion and loss of privacy;

g. money paid to, and purchasing products from, Capital One's business during the Data Breach (like interest on credit cards, minimum balance fees, and other banking fees), expenditures which Plaintiffs and Class Members would not have made shad Capital One disclosed that it lacked computer systems and data security practices adequate to safeguard consumers' PII;

h. out-of-pocket expenses and the value of their time reasonably incurred to ferret out and remedy or mitigate the effects of the Data Breach;

i. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;

j. loss of use of, and access to, their funds, and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, resulting in missed payments on bills and loans, late charges and fees, and the ensuing adverse effects on their credit including adverse credit notations; and

k. the loss of productivity and value of the time needed to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including searching for and finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all

such issues resulting from the Data Breach.

110. While Plaintiffs' and Class Members' PII has been stolen, Capital One continues to hold their PII. Because Capital One has demonstrated an inability to prevent a breach, Plaintiffs and Class Members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

111. Plaintiffs bring this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23, seeking damages and equitable relief on behalf of the following nationwide Class ("Class", to include both subclasses) for which Plaintiff seeks certification:

> All natural persons residing in the United States and whose PII was disclosed in the Data Breach.

112. Plaintiffs also bring this action on behalf of a subclass of consumers (the "Denied Subclass") defined as follows:

> All natural persons residing in the United States, whose PII was disclosed in the Data Breach, and who applied for Capital One credit card products from 2005 through 2019, but were not approved and/or did not receive the credit card.

113. Plaintiffs also bring this action on behalf of a subclass of consumers (the "Identity Theft Subclass") defined as follows:

> All natural persons residing in the United States, whose PII was disclosed in the Data Breach, about whom Capital One's records show that an application for a Capital One credit card product was received from 2005 through 2019, but did not in fact apply for the credit card.

114. Excluded from the Class are employees of Capital One; any parent, affiliate, or subsidiary of Capital One; employees of any entity in which Capital One has a controlling interest; any of Capital One's officers or directors; or any successor or assign of Capital One. Also excluded

are any Judge or court personnel assigned to this case and Members of their immediate families, all attorneys representing the Plaintiffs and any employees or immediate family members of such attorneys.

115. **Numerosity. Fed. R. Civ. P. 23(a)(l).** The Class is so numerous that joinder of all Members is impracticable. While Plaintiffs do not know the exact number of the Members of the Class. Plaintiffs believe the Class contains approximately 100 million people. Class Members may be identified through objective means using Capital One's records. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, social media, and/or published notice.

116. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** This action involves common questions of law and fact exist as to all Members of the Class, and predominate over any questions affecting individual Members of the Class. Such questions of law and fact common to the Class include, but are not limited to:

a. Whether Capital One had a duty to adequately protect PII from consumers who applied for Capital One credit card products;

b. Whether Capital One breached that duty by acts or omissions;

c. Whether the breach proximately caused damages to Plaintiffs and Class Members;

d. Whether and when Capital One knew or should have known of the susceptibility of its computer systems to a data breach;

e. Whether Capital One's security measures to protect its computer systems were reasonable in light of the FTC data security recommendations and best practices recommended by data security experts;

f. Whether Capital One was negligent in failing to implement reasonable and adequate security procedures and practices to protect the information it collected and stored from consumers who applied for Capital One credit card products;

g. Whether Capital One's conduct, practices, actions, and/or omissions constituted

unfair or deceptive trade practices;

h. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of Capital One's failure to reasonably protect its computer systems and data network; and

i. The relief, including injunctive relief, to which Plaintiffs and Class Members are entitled.

117. **Typicality. Fed. R. Civ. P. 23(a)(3).** Plaintiffs' claims are typical of the claims of the Members of the Class. Plaintiffs are consumers who provided PII to in order to apply for Capital One credit card products and had their PII compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class Members, and Plaintiffs seek relief consistent with the relief of the Class Members.

118. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Plaintiffs are adequate representatives of the Class because Plaintiffs are Members of the Class and are committed to pursuing this matter against Capital One to obtain relief for the Class. Plaintiffs have no conflicts of interest with Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions, including privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class' interests. Plaintiffs' claims arise out of the same common course of conduct giving rise to the claims of the other Members of the Class. Plaintiffs' interests are coincident with, and not antagonistic to, those of the other Members of the Class.

119. Plaintiff Yancey is a member of the Identity Theft subclass.

120. Plaintiff DeLeon is a member of the Denied subclass.

121. **Superiority. Fed. R. Civ. P. 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no difficulties exist that are likely to impact the management of this class action. The quintessential purpose of the class action device is to permit litigation against wrongdoers even when damages to individual

plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Capital One, and thus, individual litigation to redress Capital One's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system because of the millions of cases that would need to be filed and litigated. Individual litigation also creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action mechanism presents far fewer management difficulties and provides the benefits of a single adjudication using common proof and before a single court.

122. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Capital One, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate for the Class.

123. Similarly, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues are set forth in Paragraphs 1 through 118 above.

124. Finally, all Members of the proposed Class are readily ascertainable. Capital One has access to information regarding the applications from consumers for the span of time from 2005 through 2019 and the consumers affected by the Data Breach. Using this information, Class Members can be identified, and their contact information ascertained for the purpose of providing notice to the Class. Capital One also retains records as to applicants who were denied sufficient to identify and ascertain membership in the Denied Subclass. The national consumer reporting

agencies, Capital One and other available sources retain information sufficient to identify individuals who were victims of Identity Theft and did not in fact apply for the subject Capital One product.

FIRST CLAIM FOR RELIEF
Negligence (For the Class)

125. Plaintiffs restate and reallege the above paragraphs as if fully set forth herein.

126. Capital One demanded and took possession of Plaintiffs and the Class Members' PII, meaning Capital One then had a duty to exercise reasonable care in protecting that information from unauthorized access or disclosure. Capital One further had a duty to destroy Plaintiffs' and Class Members' PII within an appropriate amount of time after it was no longer required by Capital One, in order to mitigate the risk of such stale PII being compromised in the Data Breach.

127. Upon accepting and storing Plaintiff's and Class Members' PII in its computer systems and networks, Capital One undertook and owed a duty of care to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard Plaintiffs and Class Members' PII and to use commercially-reasonable methods to do so. Capital One knew that the PII was private, personal, and confidential, and should be protected.

128. Capital One owed a duty of care not to subject Plaintiffs and Class Members, along with their PII, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

129. Capital One owed a duty of care to Plaintiffs and Class Members to quickly detect a data breach and to timely act on warnings about data breaches.

130. These duties arose from Capital One's relationship to Plaintiffs and Class Members and from industry custom.

131. Capital One, through its actions and inactions, unlawfully breached duties to Plaintiffs and Class Members by failing to implement standard industry protocols and to exercise reasonable care to secure and keep private the PII entrusted to it.

132. Capital One, through its actions and omissions, allowed unmonitored and unrestricted access to unsecured PII.

133. Through its actions and omissions, Capital One failed to provide adequate supervision and oversight of the PII with which it was entrusted, despite knowing the risk and foreseeable likelihood of a breach and misuse, which permitted unknown third parties to gather Plaintiffs and Class Members' PII, misuse that PII, and intentionally disclose it to unauthorized third parties without consent.

134. Capital One knew or should have known the risks inherent in collecting and storing PII, the importance of adequate security and the well-publicized data breaches within the financial services industry.

135. Capital One knew or should have known that its data systems and networks did not adequately safeguard Plaintiffs and Class Members' PII.

136. Due to Capital One's knowledge that a breach of its systems would damage millions of its customers like Plaintiff and Class Members, Capital One had a duty to adequately protect its data systems and the PII contained thereon.

137. Capital One had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust Capital One with their PII was predicated on the understanding that Capital One demanded the PII and therefore would take adequate security precautions to safeguard that information. Moreover, only Capital One had the ability to protect its systems and the PII stored on those systems from attack.

138. Capital One's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PII. Capital One's misconduct included failing to: (1) secure its computer systems, despite knowing their vulnerabilities; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

139. Capital One also had independent duties under federal laws that required Capital One to reasonably safeguard Plaintiffs' and Class Members' PII, and promptly notify them about the Data Breach.

140. Capital One breached its duties to Plaintiffs and Class Members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Customer Data;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs and Class Members' PII before and after learning of the Data Breach;

d. by failing to comply with industry standard data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiffs and Class Members' PII had been improperly acquired or accessed.

141. Through Capital One's acts and omissions described in this Complaint, including Capital One's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Capital One unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs and Class Members' PII while it was within Capital One's possession or control.

142. The law further imposes an affirmative duty on Capital One to timely disclose the unauthorized access and theft of Plaintiffs' and Class Members' PII, so that Plaintiffs and Class Members can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

143. Capital One breached its duty to notify Plaintiffs and Class Members of the unauthorized access to their PII by waiting to notify Plaintiffs and Class Members, and then by failing to provide Plaintiffs and Class Members sufficient information regarding the breach.

144. Through Capital One's acts and omissions described in this Complaint, including Capital One's failure to provide adequate security and its failure to protect Plaintiffs' and Class Members' PII from being foreseeably captured, accessed, disseminated, stolen, and misused, Capital One unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' PII while it was within Capital One's possession or control.

145. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Capital One prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

146. Upon information and belief, Capital One improperly and inadequately safeguarded Plaintiffs' and Class Members' PII in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Capital One's failure to take proper security measures to protect sensitive PII as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' PII.

147. Capital One's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to

conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class Members' PII; and failing to provide Plaintiffs and Class Members with timely and sufficient notice that their sensitive PII had been compromised.

148. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint

149. Capital One's failure to exercise reasonable care in safeguarding PII by adopting appropriate security measures, including proper encryption storage techniques, was the direct and proximate cause of Plaintiffs' and Class Members' PII being accessed and stolen through the data breach.

150. Capital One breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

151. As a result of Capital One's breach of duties, Plaintiffs and the Class suffered damages including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of other forms of damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

SECOND CLAIM FOR RELIEF
Negligence *Per Se* (For Class)

152. Plaintiffs restate and reallege the above paragraphs as if fully set forth herein.

153. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Capital One, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Capital One's duty in this regard.

154. Capital One violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII, and not complying with applicable industry standards, as described in detail herein. Capital One's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the immense damages that would result to Plaintiff and Class Members.

155. Capital One's violation of Section 5 of the FTC Act constitutes negligence *per se.*

156. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

157. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

158. As a direct and proximate result of Capital One's negligence *per se,* Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach

on their lives, including, *inter alia,* by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

159. Additionally, as a direct and proximate result of Capital One's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Capital One's possession and is subject to further unauthorized disclosures so long as Capital One fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

THIRD CLAIM FOR RELIEF
Breach of Implied Contract (For the Class, excluding the Identity Theft Subclass)

160. Plaintiffs restate and reallege the above paragraphs as if fully set forth herein.

161. The allegations I this Count do not regard Plaintiff Yancey and other members of the Identity Theft Subclass.

162. Capital One solicited Plaintiffs and Class Members to apply for credit card products and demanded their PII in that process. Providing PII to Capital One was a condition for Plaintiffs and Class Members to receive credit. Plaintiffs and Class Members accepted Capital One's offers and provided their PII to Capital One to apply for Capital One credit card products.

163. When Plaintiffs and Class Members applied for Capital One credit card products, they provided their PII to Capital One as a prerequisite to obtaining credit. In so doing, Plaintiffs and Class Members on the one hand, and Capital One on the other, entered into mutually agreed-upon implied contracts pursuant to which Plaintiffs and Class Members agreed that their PII was valid, while Capital One agreed that it would use Plaintiffs and Class Members' PII in its

possession for only the agreed-upon purpose of processing the credit card product applications, and no other purpose.

164. Implicit in the agreement to use the PII in its possession for only the agreed-upon application and no other purpose was the obligation that Capital One would use reasonable measures to safeguard and protect the PII of Plaintiffs and Class Members in its possession.

165. By accepting PII for credit card product applications, Capital One assented to and confirmed its agreement to reasonably safeguard and protect Plaintiffs' and Class Members' PII from unauthorized disclosure or uses and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and/or compromised.

166. Plaintiffs and Class Members would not have provided and entrusted their PII to Capital One to apply for the Capital One credit card products in the absence of this implied contract between them and Capital One.

167. Plaintiff and Class Members fully performed their obligations under the implied contracts with Capital One.

168. Capital One breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect Plaintiffs' and Class Members' PII, and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

169. Capital One breached the implied contracts it made with Plaintiffs and Class Members by failing to ensure that Plaintiffs and Class Members' PII in its possession was used only for the agreed-upon application verification and no other purpose.

170. Plaintiffs and Class Members conferred a monetary benefit on Capital One which has accepted or retained that benefit. Specifically, the credit card products typically carry annual

fees and other charges (e.g. interest) for use. In exchange, Plaintiff and Class Members should have received the services that were the subject of the transaction and should have been entitled to have Capital One protect their PII with adequate data security measures.

171. Capital One failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

172. Capital One acquired the PII through inequitable means when it failed to disclose the inadequate security practices previously alleged.

173. If Plaintiffs and Class Members had known that Capital One would employ inadequate security measures to safeguard PII, they would not have applied for the Capital One credit card products or otherwise shared their PII with Capital One.

174. As a direct and proximate result of Capital One's breaches of the implied contracts between Capital One on the one hand, and Plaintiffs and Class Members on the other, Plaintiffs and Class Members sustained actual losses and damages as described in detail above.

175. Plaintiffs and Class Members were harmed as the result of Capital One's breach of the implied contracts because their PII was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiffs and Class Members also suffered diminution in value of their PII in that it is now easily available to hackers on the dark web. Plaintiffs and the Class have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, late fees, bank fees, and other expenses relating to identity theft losses or protective measures. The Class Members are further damaged as their PII remains in the hands of those who obtained it without their consent.

176. This breach of implied contracts was a direct and legal cause of the injuries and damages to Plaintiffs and Class Members as described above.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment (For the Class)

177. Plaintiffs restate and realleges the above paragraphs as if fully set forth herein.

178. Plaintiffs and Members of the Class conferred a monetary benefit on Capital One. Specifically, they provided and entrusted their PII to Capital One.

179. In exchange, Plaintiffs and Class Members should have been entitled to have Capital One protect their PII with adequate data security.

180. Capital One appreciated, accepted, and retained the benefit bestowed upon it under inequitable and unjust circumstances arising from Capital One's conduct toward Plaintiffs and Class Members as described herein: Plaintiffs and Class Members conferred a benefit on Capital One and accepted or retained that benefit. Capital One used Plaintiffs' and Class Members' PII for business purposes.

181. Capital One failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiff and Class Members provided.

182. Capital One acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged, as well as failing to destroy or otherwise purge the PII from its computer systems after Capital One no longer had a legitimate business purpose to maintain that PII.

183. If Plaintiffs and Class Members knew that Capital One would not secure their PII using adequate security, they would not have applied for Capital One credit card products.

184. Plaintiffs and Class Members have no adequate remedy at law for the injuries they suffered due to Capital One's conduct.

185. Under the circumstances, it would be unjust for Capital One to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred on it.

186. Under the principles of equity and good conscience, Capital One should not be permitted to retain the PII belonging to Plaintiffs and Class Members because Capital One failed to implement the data management and security measures that industry standards mandate.

187. Capital One should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them. In the alternative, Capital One should be compelled to refund the amounts that Plaintiff and Class Members overpaid for security they did not receive.

FIFTH CLAIM FOR RELIEF
Declaratory Judgment (For the Class)

188. Plaintiffs restate and reallege the above paragraphs as if fully set forth herein.

189. As previously alleged, Plaintiffs and Class Members entered into an implied contract that required Capital One to provide adequate security for the PII it collected from their applications for Capital One credit card products. As previously alleged, Capital One owes duties of care to Plaintiff and Class Members that require it to adequately secure PII.

190. Capital One still possesses PII pertaining to Plaintiffs and Class Members.

191. Capital One has not announced or otherwise notified Plaintiff and Class Members that their PII are sufficiently protected or, more importantly, expunged from Capital One's servers so as to prevent any further breaches or compromises.

192. Indeed, Capital One has stated that PII from Capital One credit card product applications submitted as far back as 2005 is subject to the Data Breach.

193. Accordingly, Capital One has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that Capital One's lax approach to data security has become public, the PII in its possession is more vulnerable than before.

194. Actual harm has arisen in the wake of the Data Breach regarding Capital One's contractual obligations and duties of care to provide data security measures to Plaintiffs and Class Members.

195. Plaintiffs therefore seek a declaration that: (a) Capital One's existing data security measures do not comply with its contractual obligations and duties of care; and (b) in order to comply with its contractual obligations and duties of care, Capital One must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Capital One's systems on a periodic basis, and ordering Capital One to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of Capital One is compromised, hackers cannot gain access to other portions of Capital One's systems;

e. purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

f. conducting regular database scans and security checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their

financial and personal information to third parties, as well as the steps Capital One's customers should take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, respectfully seek from the Court the following relief:

a. Certification of the Class as requested herein under Federal Rule of Civil Procedure 23;

b. Appointment of Plaintiffs as Class Representatives and their undersigned Counsel as Class counsel;

c. Award Plaintiffs and Members of the proposed Class damages;

d. Award Plaintiffs and Members of the proposed Class equitable, injunctive and declaratory relief, including the enjoining of Capital One's insufficient data protection practices at issue herein and Capital One's continuation of its unlawful business practices as alleged herein;

e. An order declaring that Capital One's acts and practices with respect to the safekeeping of PII were negligent;

f. Award Plaintiffs and Members of the proposed Class pre-judgment and post-judgment interest as permitted by law;

g. Award Plaintiffs and Members of the proposed Class reasonable attorneys' fees and costs of suit, including expert witness fees; and

h. Award Plaintiffs and Members of the proposed Class any further relief the Court deems proper.

TRIAL BY JURY IS HEREBY DEMANDED.

Dated: August 2, 2019

Respectfully submitted,

PLAINTIFFS,

By: /s/ *Leonard A. Bennett*

Leonard A. Bennett, VSB #37523
Email: lenbennett@clalegal.com
Elizabeth W. Hanes, VSB #75574
Email: elizabeth@clalegal.com
Craig C. Marchiando, VSB #89736
Email: craig@clalegal.com
CONSUMER LITIGATION ASSOCIATES, P.C.
763 J. Clyde Morris Boulevard, Suite 1-A
Newport News, Virginia 23601
Telephone: (757) 930-3660
Facsimile: (757) 930-3662

Matthew J. Erausquin VSB #65434
Tara B. Keller VSB #91986
CONSUMER LITIGATION ASSOCIATES, P.C.
1800 Diagonal Road, Ste. 600
Alexandria, Virginia 22314
(703) 273-7770 - Telephone
(888) 892-3512 - Facsimile
Email: matt@clalegal.com
Email: tara@clalegal.com

Kristi C. Kelly, VSB #72791
Email: kkelly@kellyguzzo.com
Andrew J. Guzzo, VSB #82170
Email: aguzzo@kellyguzzo.com
Casey S. Nash, VSB #84261
Email: casey@kellyguzzo.com
KELLY GUZZO, PLC
3925 Chain Bridge Road, Suite 202
Fairfax, Virginia 22030
Telephone: (703) 424-7572
Facsimile: (703) 591-0167

Charles B. Molster, VSB #23613
Email: cmolster@molsterlaw.com
LAW OFFICES OF CHARLES B. MOLSTER, III, PLLC
2141 Wisconsin Avenue, N.W., Suite 202
Washington, D.C. 20007
Telephone: (202) 787-1312

Attorneys for Plaintiffs and Proposed Class